

# Web Portal Domain Authentication

This section allows to configure how the web portal can be accessed.

## Domain Authentication

Libraesva ESG relies on a per domain authentication mechanism.

From this tab you can define how each hosted domain is authenticated when logging in on the Libraesva ESG Web Portal.

The screenshot shows the 'Web Portal Domain Authentication' configuration page in the Libraesva ESG web interface. The page has a green header bar with the title 'Web Portal Domain Authentication'. Below the header, there is a description: 'Libra Esva Web Portal Domain Authentication allows to define per domain authentication scheme to access the Libra Esva web portal.' The main content area is divided into two sections. The top section is a table with columns 'Domain' and 'Authentication Method'. It lists four domains: 'esva-spamtest.it', 'esvaspamtest.com', 'example.com', and 'test.it', all using 'Local DB Authentication'. The bottom section is a detailed view for the 'esva-spamtest.it' domain, showing a table of 'Domain Associated Sets'. This table has columns: 'Type', 'Description', 'Host', and 'Authenticate Users'. It lists six entries: three 'POP3' entries with 'POP3 Test' description, and three 'POP3' entries with 'pop' description, all with 'Yes' for 'Authenticate Users'. There is also an 'IMAP' entry with 'Yes' for 'Authenticate Users'. The page includes navigation tabs at the top: 'Home', 'System', 'Reports', 'Quarantine', and 'Search'. There are also dropdown menus for 'Appliance', 'Mail Transport', 'Content Analysis', 'Authentication', and 'High Availability'. The bottom of the page shows a search bar, a page number '25', and a display range 'Displaying rows 1 to 4 of 4'.

LIBRAESVA  
email security virtual appliance

Home System Reports Quarantine Search

Appliance Mail Transport Content Analysis Authentication High Availability

### Web Portal Domain Authentication

Libra Esva Web Portal Domain Authentication allows to define per domain authentication scheme to access the Libra Esva web portal.

Search Help

| Domain           | Authentication Method   |
|------------------|-------------------------|
| esva-spamtest.it | Local DB Authentication |
| esvaspamtest.com | Local DB Authentication |
| example.com      | Local DB Authentication |
| test.it          | Local DB Authentication |

Domain Associated Sets

| Type | Description | Host | Authenticate Users |
|------|-------------|------|--------------------|
| POP3 | POP3 Test   |      | Yes                |
| POP3 |             |      | Yes                |
| POP3 |             |      | Yes                |
| POP3 | pop         |      | Yes                |
| POP3 | pop         |      | Yes                |
| IMAP |             |      | Yes                |

Displaying rows 1 to 6 of 6

25 1 Displaying rows 1 to 4 of 4

You can choose from one of the followings:

- **“No Access”** means that the users belonging to this domain will be locked out from the web interface.
- **“Local DB Authentication”** means that user’s password is stored locally on ESG DB. Users are created locally from *System->User Management*
- **“Ldap Authentication”** means that user’s password is stored on a LDAP server. The login username has to be the user main email address as mapped in the LDAP set. The email domain is used to correctly identify the user associated LDAP server in LDAP dataset List. At least one LDAP set must be defined and active.
- **“Pop3 Authentication”** means that user’s password is stored on the POP3 server. Obviously, also in this case, the login username has to be the user email address. At least one POP3 set must be defined and active.
- **“IMAP Authentication”** means that user’s password is stored on the IMAP server. Obviously, also in this case, the login username has to be the user email address. At least one IMAP set must be defined and active.
- **“Office 365 Authentication”** means that user’s password is stored on the Office365 Tenant. Obviously, also in this case, the login username has to be the user email address. At least one Office365 must be defined and active.
- **“Google Authentication”** means that user’s password is stored on the Gsuite Tenant. Obviously, also in this case, the login username has to be the user email address. At least one Google Configuration must be defined and active.

When choosing any authentication method other than Local, it’s handy to see which sets are already associated to each domain. By clicking the + icon on the left you can expand and check LDAP, POP3, IMAP sets defined for the domain.

×**NOTE:** default authentication scheme is always Local.

## Login Authorized Networks

This section permits to restrict the portal access login, making it working only if the request originates from a definite set of networks or IPs.

## Web Portal Authentication

Libra Esva Web Portal Authentication allows to define access policies the Libra Esva web portal.

Domain Authentication Login Authorized Networks

### Login Authorized Networks

This functionality permits the Web Portal Login only from a definite set of source networks.  
**By default logins are permitted from any network.**  
 Each User Type (Administrator, Domain Admin, User) has it's own permissions.

#### Login Authorized Networks

+ New Search Export Delete selected

|  | Permitted Network | User Role |
|--|-------------------|-----------|
|--|-------------------|-----------|

No records found

Search Previous Next Refresh

To restrict web portal access:

1. Click **New**
2. Enter the permitted source network
3. Specify the user role: Administrator, Domain Admin, User
4. Click **Save**

For example to restrict admin access only if the portal is accessed from the IP 1.2.3.4 enter:

**Permitted Network: 1.2.3.4/32**

**User Role: Administrators**

×**NOTE:** by default logins are permitted from any network, for all user types.